

BOLLETTINO DI SICUREZZA XEROX XRX06-004

Aggiornamento cumulativo che risolve varie vulnerabilità delle funzioni di sicurezza.

Le versioni del software di sistema 12.050.03.000, 14.050.03.000 o 13.050.03.000, a seconda che il prodotto sia un WorkCentre® o un WorkCentre® Pro, sono un aggiornamento delle versioni 12.027.24.000, 14.027.24.000 e 13.027.24.000, rispettivamente, e comprendono correzioni al software di sistema. Consultare l'Appendice A delle istruzioni per l'installazione della patch per informazioni su come ottenere il software di sistema *.50.03.000¹.

Si consiglia ai clienti di aggiornare il software di sistema caricato sul dispositivo alla versione 12.050.03.000, 14.050.03.000 o 13.050.03.000, rispettivamente. La tabella che segue indica la versione corrispondente del controller di rete per ogni software di sistema.

Versione SW di sistema	Versione controller di rete
12.050.03.000.	040.010.01172
13.050.03.000.	040.010.51172
14.050.03.000.	040.010.11172

Contesto

Le versioni 12.050.03.000, 14.050.03.000 e 13.050.03.000 del software di sistema sono release di mantenimento che comprendono soluzioni a problemi di sicurezza delle versioni 12.027.24.000, 14.027.24.000 e 13.027.24.000 del software di sistema, rispettivamente. L'aggiornamento comprende soluzioni alle seguenti vulnerabilità delle funzioni di sicurezza presenti nel codice del controller di rete/ESS e del server Web MicroServer:

- L'autenticazione richiesta dall'interfaccia utente Web può essere aggirata.
- Avviso "US-CERT Technical Cyber Security Alert TA04-174A".
- La versione Samba deve essere aggiornata affinché varie vulnerabilità possano essere eliminate.
- L'agente SNMP non restituisce un errore per gli oggetti protetti da scrittura.
- Impossibile abilitare o generare le trap per la mancata autenticazione SNMP.
- Vulnerabilità del controller di rete: attacco XSS tramite metodo "HTTP TRACE".
- Lo script PS allegato provoca l'interruzione di ops3-dmn con core dump; attacco DOS.
- La condivisione "Homes" di SMB è visibile.
- È possibile consultare il file system SMB.
- È possibile eseguire dei download anonimi dal registro di controllo.
- Problemi alle funzioni di sicurezza HTTP.
- Aggiramento delle funzioni di protezione e avvio di Alchemy tramite un thumb drive USB (o metodo alternativo).
- La funzione di scansione "Convalida certificato SSL archivio" non controlla FQDN.
- Alcuni privilegi di accesso ai file andrebbero resi più severi.
- Sicurezza di Linux - La vulnerabilità del kernel CAN-2003-0643 deve essere risolta - problema socket.
- La porta 443 è sempre attiva - errata configurazione di httpd.conf.
- Blocco della porta Postgres.
- Impossibile abilitare o generare le trap per la mancata autenticazione SNMP.
- Dopo la sovrascrittura immagini immediata (IIO) permangono dei frammenti CRITICI di dati degli utenti nel registro http.log.

¹* corrisponde a 12, 13 o 14, a seconda che il prodotto sia un WorkCentre® o un WorkCentre® Pro

- Se la sovrascrittura non viene eseguita correttamente viene scritto un messaggio di errore IIO su LUI.
- Quando si cancella un lavoro trattenuto, la sovrascrittura immagini immediata (IIO) registra un errore.
- La sovrascrittura di immagini su richiesta non viene eseguita per operazioni che riguardano oltre 2 GB di dati.

Se sfruttate, queste vulnerabilità impedirebbero un corretto funzionamento delle funzioni di protezione e un pirata informatico riuscirebbe ad accedere al sistema senza autorizzazione e a cambiarne la configurazione. Le password del cliente e dell'utente non sono a rischio.

Prodotti a rischio:

WorkCentre®	WorkCentre® Pro
232	232
238	238
245	245
255	255
265	265
275	275

Appendice A

Come ottenere il software di sistema *.50.03.000

Per ottenere la versione generica più recente:

- a) Mediante un browser accedere al sito www.xerox.com.
- b) Selezionare il collegamento "Supporto e Driver".
- c) Selezionare "Multifunzione".
- d) Selezionare "WorkCentre" o "WorkCentre Pro", a seconda del modello che si possiede.
- e) Individuare il collegamento corrispondente al proprio modello di WorkCentre.
- f) Selezionare "Driver e Download".
- g) Selezionare il collegamento "Aggiornamenti per i prodotti".
- h) Selezionare il collegamento "System software version *.50.03.000 install instructions" e stampare il documento (oppure salvarlo).
- i) Selezionare il collegamento "System Software Upgrade Version *.50.03.000" e salvare il file sul computer.
- j) Dopo aver scaricato il file, estrarne il contenuto sul desktop.
- k) Consultare il documento dc06cc0406.pdf incluso nel pacchetto scaricato per informazioni sull'aggiornamento del dispositivo.
- l) Consultare il file delle istruzioni per l'installazione del software di sistema ("System Software Install Instructions") salvato.
- m) Aggiornare il dispositivo.
- n) Ritornare alla sezione "Installazione della patch".

Declinazione di responsabilità

Le informazioni contenute in questo documento Xerox sono fornite "così come sono" senza alcuna garanzia. Xerox Corporation non riconosce alcuna garanzia, espressa o implicita, comprese le garanzie di commerciabilità e idoneità a uno scopo specifico. In nessun caso Xerox Corporation potrà essere ritenuta responsabile di danni di qualsiasi tipo risultanti dall'uso dell'utente o dal mancato rispetto delle informazioni fornite in questo documento Xerox, inclusi danni speciali, diretti, indiretti, incidentali, consequenziali o perdita

di profitti aziendali, anche nel caso in cui Xerox Corporation sia stata informata della possibilità di tali danni. Alcuni paesi non consentono l'esclusione o la limitazione della responsabilità per i danni consequenziali, di conseguenza le limitazioni di cui sopra potrebbero non essere applicabili.